informacijski inženjering

Oracle Label Security

Zoran Jovanović
tehnički direktor

Uvod

- OLS koncepti
- Labele za klasifikaciju podataka
- Korištenje OLS
- Implementacija
- Instaliranje OLS
- Primjer implementacije OLS
- Zaključak

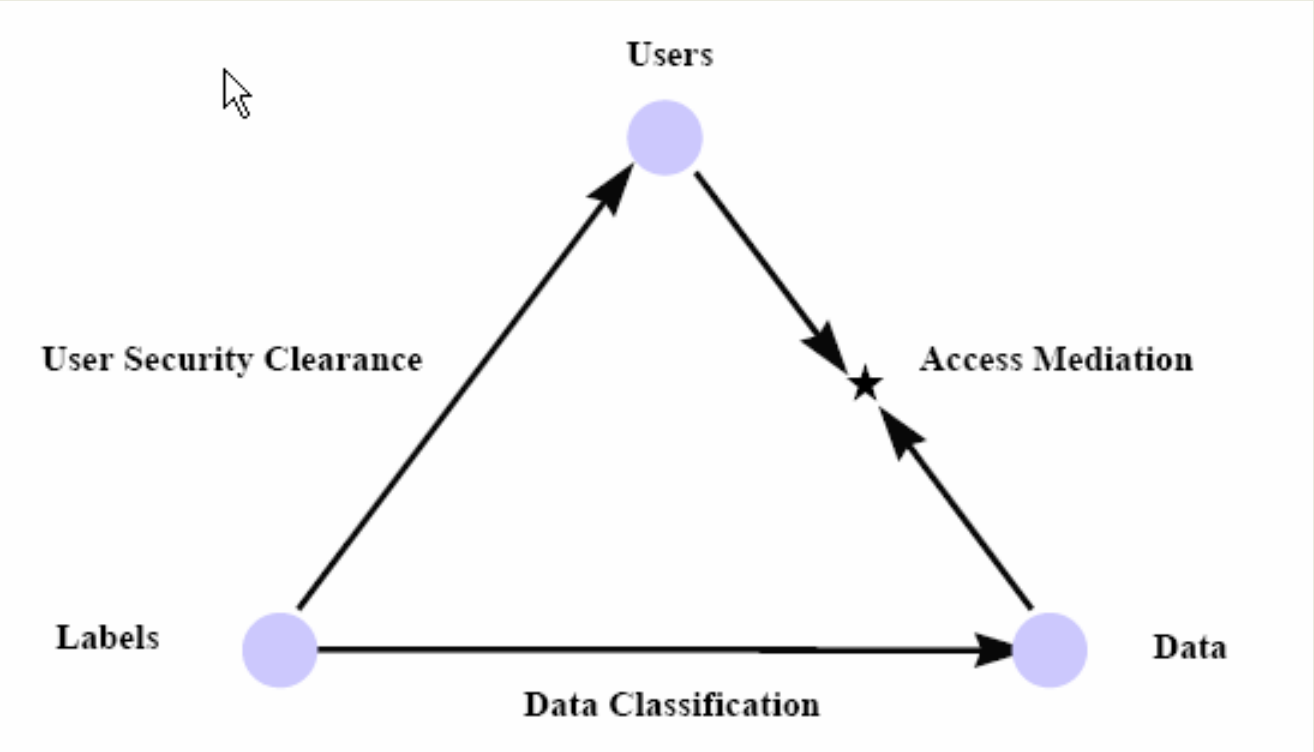
OLS koncepti

- sigurnosna opcija Oracle servera Enterprise Edition
- omogućava dodjeljivanje klasifikacijskih labela osjetljivim podacima
- upravljanje korisničkog pristupa do osjetljivih podataka
- omogućava ispunjavanje različitih zahtjeva za klasifikaciju podataka
- uspostavljanja sigurnosti pristupa na više razina
- autorizacijski mehanizam definira maksimalne i minimalne razine osjetljivosti podataka do kojih korisnik može pristupiti

OLS koncepti

- Autorizacijski mehanizam se može proširiti pored razina osjetljivosti podataka i na dodatne komponente a to su odjeljci i grupe
- Standardnim mehanizmom objektnih i sistemskih prava Oracle omogućava definiranje prava pristupa do pojedinih objekata u bazi
- OLS dodaje još dodatne autorizacijske mehanizme koji, mehanizmom medijacije pristupa, omogućavaju ograničavanje prava pristupa korisnika do privatnih i povjerljivih informacija

OLS koncepti
medijacija pristupa



OLS koncepti

- OLS koristi koncept policy radi grupiranja definiranih labela za klasifikaciju podataka i pridruženih autorizacija za pristup
- Više policy može biti definirano u jednoj bazi
- više policy može biti primijenjeno na jednu tablicu
- upravljanje sa policy može biti centralizirano unutar Oracle Identity Management
- Temeljem labela za klasifikaciju podataka određuje se kojim slogovima podataka će pojedini korisnici moći pristupiti

OLS koncepti

- labele se sastoje od tri komponente: hijerarhijska razina klasifikacije, odjeljak i grupa pri čemu je samo prva komponenta obavezna
- Razina klasifikacije je hijerarhijska komponenta koja označava osjetljivost podataka
- Odjeljak nije hijerarhijska komponenta labele. Odjeljci se definiraju da bi se podaci razdvojili
- Grupa je komponenta labele koja se koristi da bi se označilo vlasništvo za svaki od slogova podataka i one se mogu definirati hijerarhijski
- definiramo strukturu grupa i podgrupa kojima su one nadređene

OLS koncepti

- Vanjski prikaz labela za klasifikaciju podataka može se sastojati od tri komponente razdvojene dvotočkom.
- Na primjer labela „Povjerljivo:Kadrovska:Dalmacija“ se sastoji od slijedećih komponenti:
  - Razina = Povjerljivo
  - Odjeljak = Kadrovska
  - Grupa = Dalmacija
- Interno, OLS koristi notaciju tagova za labele za predstavljanje svake jednoznačne labele
- svakom slogu podataka se u dodatnu kolonu upisuje label tag koji se koristi u postupku medijacije pristupa

Korištenje OLS

- Prije implementacije OLS u Oracle bazi potrebno je analizirati aplikacije koje će ga koristiti
- U postupku analize treba odrediti slijedeće:
  1. Analizirati aplikacijske sheme da bi odredili tablice na koje treba primijeniti OLS policy
  2. analizirati podatke u tablicama za koje ćemo definirati OLS policy i definirati razine osjetljivost podataka
  3. Odjeljci se najčešće definiraju i koriste u vladinim i vojnim institucijama
  4. Grupe su komponente labela koje se koriste za upravljanje pristupom do podataka po kriteriju organizacije, regije ili vlasništva nad podacima

Korištenje OLS

5. Ako se slogu podataka dodijeli labela osjetljivosti podataka koja uključuje odjeljke i grupe tada autorizacija korisnika koji želi čitati slog podataka mora sadržavati:
   - razinu koja je viša ili jednaka razini klasifikacijske labele sloga podataka
   - sve odjeljke koji su definirani u labeli osjetljivosti podataka
   - barem jednu od grupa koje su definirane u labeli osjetljivosti podataka
6. Korisnike aplikacije moramo razdijeliti u više tipova. Na primjer korisnike možemo kategorizirati kao: standardne korisnike, korisnike sa visokom razinom prava pristupa ili administrativne korisnike

Korištenje OLS

7. OLS omogućava autorizaciju specijalnih prava koja se mogu dodijeliti korisnicima koji imaju posebne potrebe i zahtjeve
8. prije implementacije OLS, potrebno je provjeriti i dokumentirati sve prikupljene informacije.

Korištenje OLS
Metodologija analize

Tablica	Labela osjetljivosti podataka	Autorizacija korisnika (korisnička labela)			
	(*)	I	S	S:A:US	S:A,B:US,UK
Sales	I::UK	☒	☒	☒	☑
	I::US	☒	☒	☑	☑
Projects	I	☑	☑	☑	☑
	S	☒	☑	☑	☑
	S:A:US	☒	☒	☑	☑
	S:B:UK	☒	☒	☒	☑
	S:A,B:US	☒	☒	☒	☑

Razine klasifikacije podataka navedene u tabeli su:
S – Sensitive i I – Internal

Implementacija OLS

- Implementacija OLS se može izvršiti pomoću Oracle Policy Manager ili OLS PL/SQL procedura (API).
- Postupak implementacije nakon provedene gore opisane analize je slijedeći:
  1. Kreirati OLS policy
  2. Definirati komponente labele podataka: razine, odjeljci i grupe
  3. Kreirati važeće labele podataka koristeći komponente labele koje smo definirali
  4. Dodijeliti korisnicima autorizacije za pristup osjetljivim podacima i po potrebi specijalne autorizacije
  5. Primijeniti policy na tablicu sa podacima. Ako u tablici već postoje podaci tada se na početku policy primjenjuje na nju sa opcijom „no control“ što znači da su labele prazne i podaci nisu vidljivi.
  6. Nakon toga za svaki slog postojećih podataka treba kreirati odgovarajuće labele za klasifikaciju podataka
  7. Modificirati OLS policy i postaviti odgovarajuće opcije za provjeru policy-a.

Implementacija OLS
Upisivanje labela za postojeće podatke

- Kada se OLS policy sa kontrolom čitanja podataka primjeni na aplikacijsku tablicu nijedan slog podataka nije vidljiv (ne može ga se pročitati) dok se svakom slogu podataka ne pridijeli važeća labela za klasifikaciju podataka
- Kad se OLS policy primjeni na neku tablicu u toj tablici se kreira jedna dodatna kolona u koju se upisuje labela klasifikacije podataka za svaki slog. Pomoću SQL naredbe možemo ažurirati sadržaj ove dodatne kolone:

```
UPDATE SALES SET SECLAB = char_to_label : ('FINANCE','S')
WHERE REGION_ID = 104;
```

Implementacija OLS
Upisivanje labela za postojeće podatke

- Druga metoda za labeliranje postojećih podataka je da se izvrši prijava u bazu pod drugim korisničkim imenom tijekom punjenja podataka.

```
CONNECT US_SALES_MGR;
INSERT INTO SALES (Col1, Col2, Col3) VALUES ('ACME', ……);
```

- Ako policy primijenjen na tablicu **sales** sadrži i opciju LABEL_DEFAULT za provjeru policy, korisnici ne trebaju navoditi vrijednost za OLS label kolonu jer će se u tom slučaju koristiti default vrijednost ROWLABEL.
- Treća metoda je da se napiše funkcija za upisivanje labela korištenjem PL/SQL.
- Četvrta metoda za labeliranje podataka je da se napiše pohranjena procedura koja ažurira sadržaj OLS kolone u tablici na koju je primijenjen policy.

Implementacija OLS
Skrivanje OLS label kolone

- OLS zahtjeva da se kod kreiranja policy definira ime kolone u koju će se upisivati labele.
- Kad se policy primijeni na aplikacijsku tablicu kolona sa imenom koje je definirano kod kreiranja policy se kreira u toj tablici.
- OLS ima opciju za skrivanje te label kolone radi transparentnosti za postojeće aplikacije:
  - Ako je kolona skrivena ona neće biti prikazana kod izvršavanja SQL*Plus **describe** naredbe.
  - Skrivanje kolone omogućava da SQL naredbe u kojima nije navedeno ime OLS kolone ili nije navedeno ime nijedne kolone u tablici, mogu i dalje funkcionirati bez obzira na to što je u tablicu dodana nova kolona za labele
- Kolona koju OLS policy koristi za pohranjivanje labela može postojati u tablici i prije nego što OLS policy primijenimo na tu tablicu. Važno je samo to da tip te kolone mora biti definiran kao NUMBER(10).

Implementacija OLS
Oracle Policy Manager

- Oracle Policy Manager je GUI administratorski alat za administriranje OLS i Virtual Private Database.
- Ovaj alat pokrećemo tako da u komandnoj liniji na Windows ili UNIX operacijskim sustavima napišemo **„oemapp opm“**.
- Ta naredba će pokrenuti Oracle Policy Manager.
- Da bi upravljali sa OLS policy korištenjem Oracle Policy Manager-a na bazu ćemo se spojiti kao korisnik **lbacsys** ili kao drugi korisnik sa odgovarajućim pravima.

Implementacija OLS
OLS delegirana administracija

- Korisnik **lbacsys** je primarni administrator za OLS.
- Taj korisnik može autorizirati i druge korisnike baze da mogu kreirati i upravljati sa OLS policy.
- Kad se kreira OLS policy tada se automatski kreira i nova rola u bazi. Ime ove role sadrži u sebi i naziv policy u formatu „naziv_policy_DBA“:

```
CONNECT LBACSYS
EXECUTE
  SA_SYSDBA.CREATE_POLICY('HR_SECURITY','HR_LABEL');
GRANT HR_SECURITY_DBA to HR_INFOSEC;
```

Implementacija OLS
OLS delegirana administracija

- Pored toga tom korisniku moramo dodijeliti i slijedeća prava:

```
GRANT EXECUTE ON sa_components TO HR_INFOSEC;
GRANT EXECUTE ON sa_user_admin TO HR_INFOSEC;
GRANT EXECUTE ON sa_audit_admin TO HR_INFOSEC;
```

Implementacija OLS
Izuzeci kod provjere OLS policy

- Oracle Virtual Private Database (VPD) i OLS policy:
  - se ne provjeravaju kod direct path export-a.
  - se ne mogu kreirati za objekte u **sys** shemi što znači da korisnici sa privilegiranom DBA prijavom **sys** nemaju policy koji bi se provjeravao kod izvršavanja njihovih poslova.
  - Korisnici baze kojima je dodijeljeno pravo EXEMPT ACCESS POLICY, direktno ili preko role, su izuzeti od provjera VPD i OLS policy bez obzira na to koji pomoćni program koriste za ekstrakciju podataka iz baze. Ovo pravo je vrlo moćno tako da treba biti oprezan pri njegovom dodjeljivanju korisnicima.
  - Objektna prava kao što su SELECT, INSERT, UPDATE i DELETE se uvijek provjeravaju čak i za korisnike kojima je dodijeljeno pravo EXEMPT ACCESS POLICY.

Implementacija OLS

Integracija Identity Management sa Enterprise User Security

- OLS je integriran sa Oracle Identity Management kroz Enterprise User Security
- omogućava da se OLS policy i autorizacije korisnika definiraju i da se sa njima upravlja u Oracle Internet Directory (OID)
- Ove informacije se iz OID automatski propagiraju u sve baze koje su u njemu registrirane.
- Integracija OLS sa Oracle Identity Management da se autorizacija za tisuće korisnika može dodijeliti u OID i mapirati na jednu dijeljenu shemu u jednoj ili više baza koje koriste OID.
- Kada se korisnik spaja kroz Enterprise User Security dijeljenu shemu u bilo koju bazu OLS će moći inicijalizirati autorizaciju korisnika u bazi iako se korisnik ne spaja na vlastitu već dijeljenu shemu u bazi.

Implementacija OLS

Integracija Identity Management sa Enterprise User Security

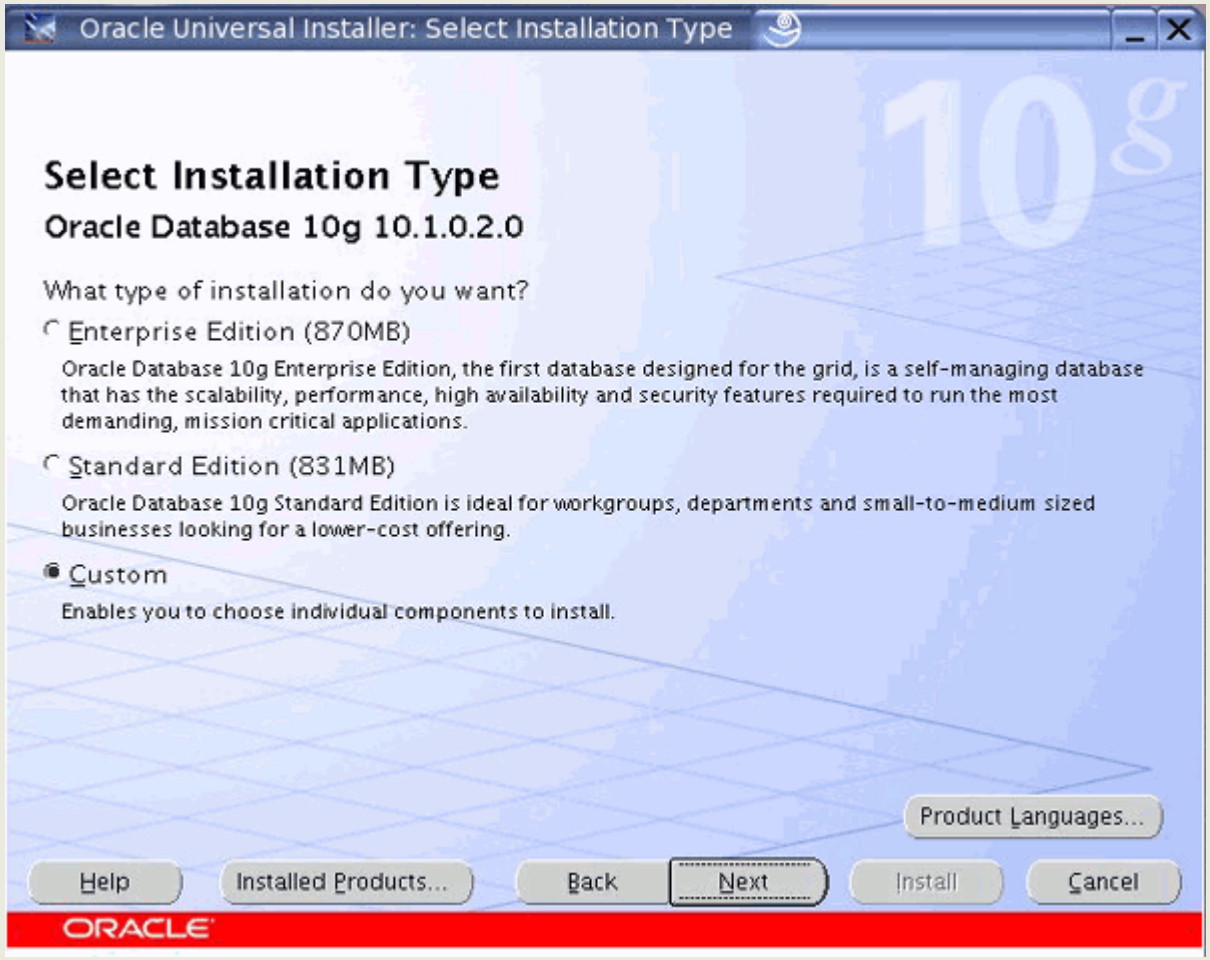
- Za aplikacije koje nisu integrirane sa Oracle Identity Management i ne koriste Enterprise User Security, korisnicima se i dalje može dodijeliti autorizacija u bazi korištenjem funkcije set_user_labels.
- Kad se OLS policy autorizacija dodjeljuje korisniku ime tog korisnika ne mora biti važeće ime korisnika u bazi već to može biti i dijeljena shema.
- OLS omogućava da autorizirani korisnik može preuzeti OLS autorizacijski profil nekog drugog korisnika.
- U slijedećem primjeru korisnik **sec_admin** će preuzeti autorizacijski profil korisnika **scott** sa OLS policy PRIVACY:

```
SQL> connect sec_admin/welcome;
SQL> execute sa_session.set_access_profile ('PRIVACY','SCOTT');
SQL> select * from emp;
```

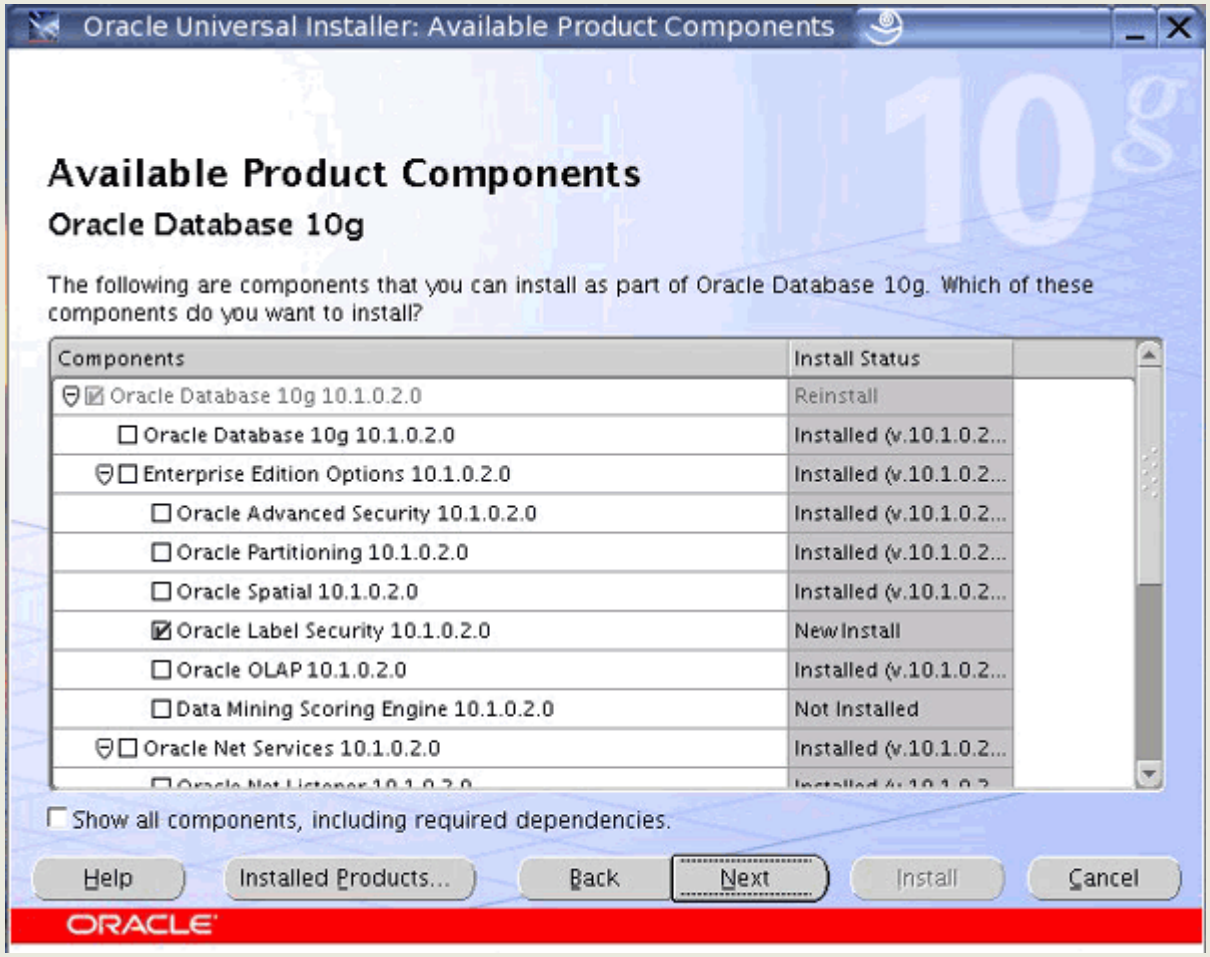
Instaliranje Oracle Label Security

- Oracle Label Security je opcija Oracle Database Enterprise Edition i po default se ne instalira kod instalacije Enterprise Edition.
- Da bi OLS instalirao potrebno je pokrenuti Oracle Universal Installer sa distribucije Oracle Server softvera i kod dijaloga Select Installation Type odabrati opciju Custom.
- Kod dijaloga Available Product Components treba kliknuti mišem i označiti kvadratić ispred retka u kojem piše Oracle Label Security.
- Nakon toga će Oracle Universal Installer instalirati sav potreban softver za podršku OLS opcije.

Instaliranje Oracle Label Security



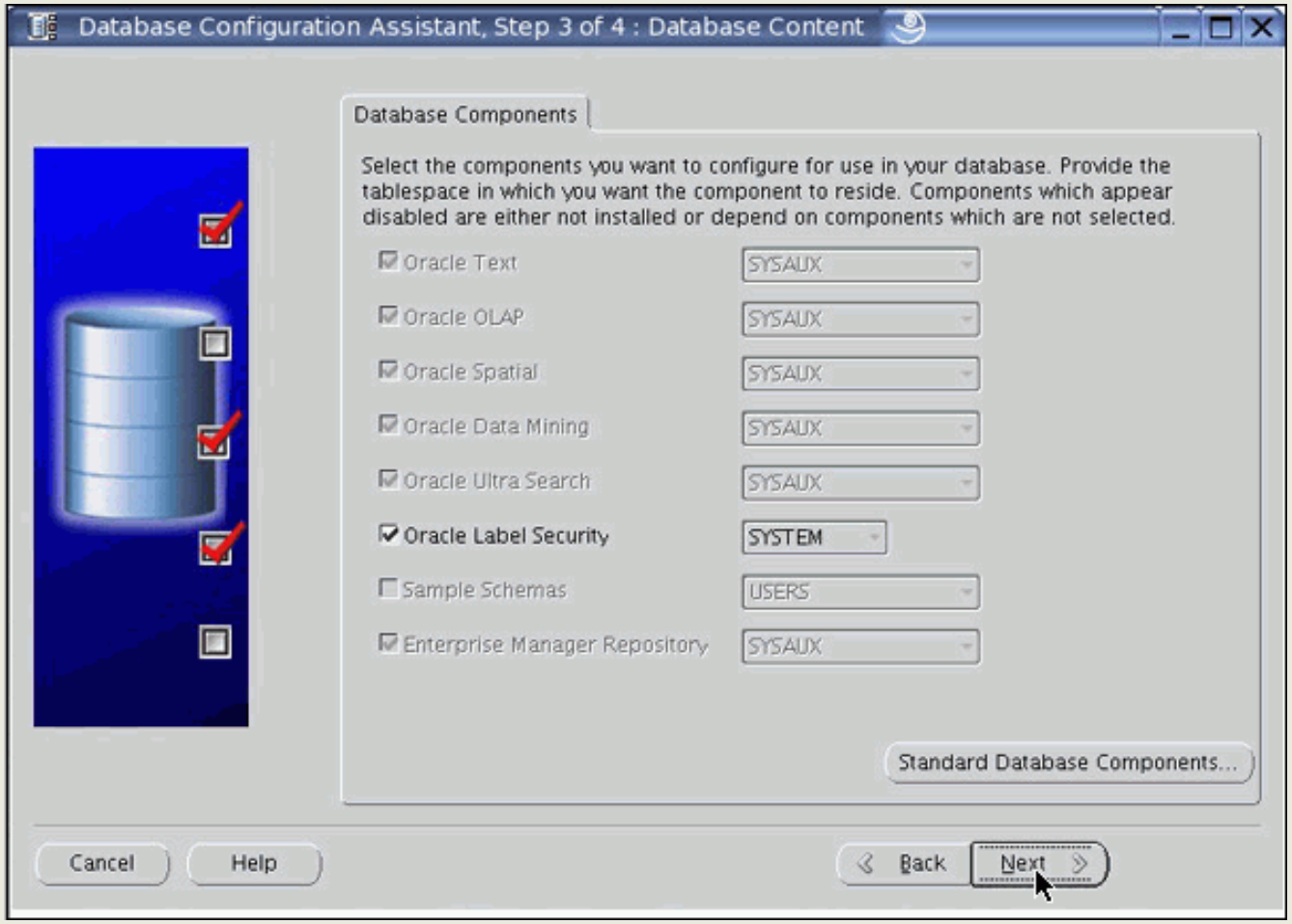
Instaliranje Oracle Label Security



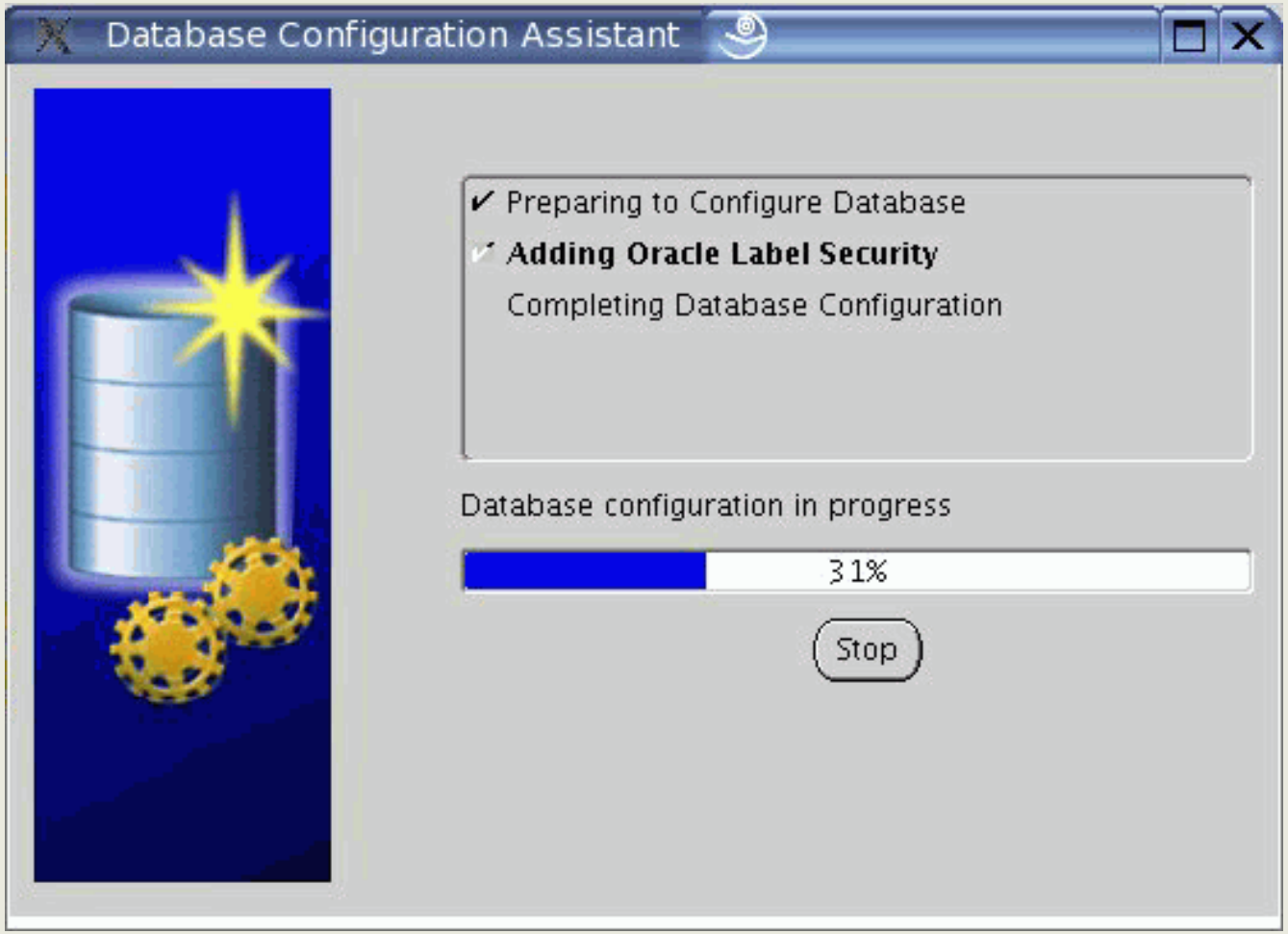
Instaliranje Oracle Label Security

- Da bi za Oracle bazu koju kreiramo mogli koristiti OLS potrebno je da kod konfiguriranja baze odaberemo ugradnju podrške za OLS u Oracle bazu.
- To možemo napraviti tako da sa Database Configuration Assistant kod kreiranja baze ili nakon što je baza kreirana (odaberemo opciju Configure Database Options) u dijalogu Database Components odaberemo opciju Oracle Label Security.
- Nakon toga će Database Configuration Assistant u bazi kreirati korisnika LBACSYS i u njegovoj shemi će kreirati sve objekte koji su potrebni za podršku OLS.
- Ovaj korisnik se kreira sa statusom locked i expired a početna lozinka mu je LBACSYS.
- Da bi mogli koristiti OLS trebamo napraviti unlock korisnika LBACSYS i kod prve prijave pod njegovim korisničkim imenom moramo mu promijeniti lozinku.

Instaliranje Oracle Label Security



Instaliranje Oracle Label Security



Primjer implementacije OLS

- implementaciju OLS na primjeru jedne prodajne organizacije.
- Prodaja u toj organizaciji je podijeljena u 5 regija tako da za svaku regiju postoji regionalni menadžer koji je zadužen za prodaju u svojoj regiji i u centrali tvrtke postoji menadžer koji je zadužen za koordinaciju prodaje cijele tvrtke.
- U ovom primjeru ću pokazati kako se pomoću OLS može ograničiti pravo dostupa do podataka tako da svaki regionalni menadžer može vidjeti samo podatke koji se odnose na njegovu vlastitu regiju a samo menadžer u centrali tvrtke može vidjeti prodajne podatke za cijelu tvrtku.

Primjer implementacije OLS

Sigurnosne grupe			
Group ID	**Short Name**	**Long Name**	**Parent**
0	T	Top of Sales Force Hierarchy	(none)
10	NE	Northeastern Sales Region	T
20	SE	Southeastern Sales Region	T
30	CN	Central Sales Region	T
40	SW	Southwestern Sales Region	T
50	NW	Northwestern Sales Region	T

Primjer implementacije OLS

Odjeli u tvrtki – odjeljci za OLS		
Compartment ID	**Short Name**	**Long Name**
100	AC	Accounting
200	SA	Sales Administration
300	HR	Human Resources
400	OP	Operations
500	OE	Order Entry

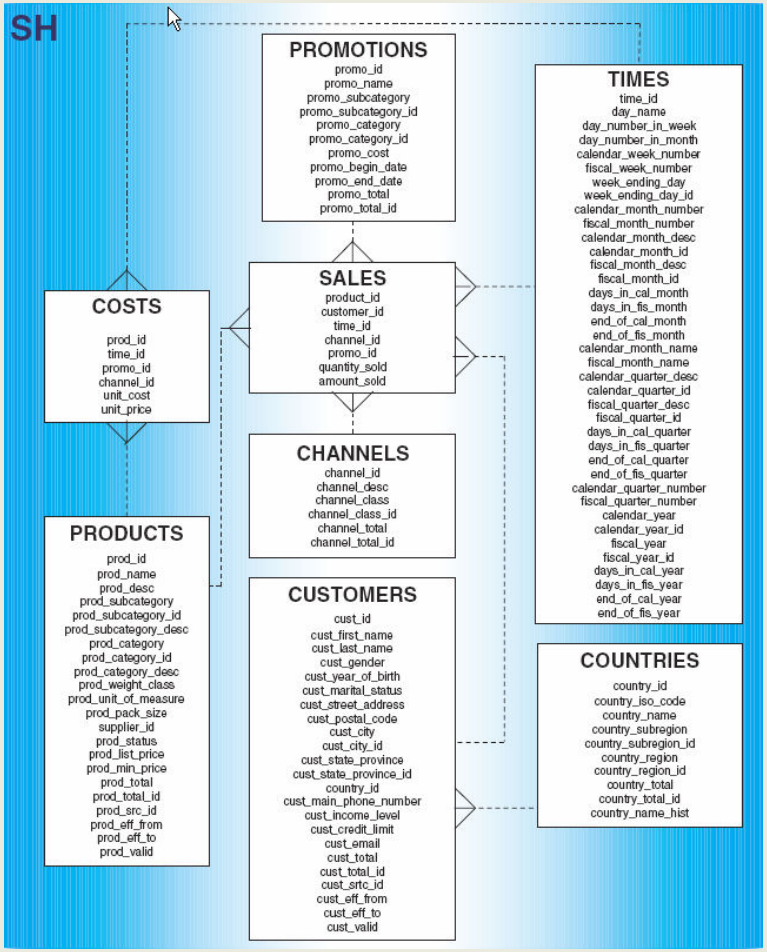
Primjer implementacije OLS

Razine osjetljivosti podataka		
Level ID	**Short Name**	**Long Name**
1000	UN	Unsecured
3000	CW	CompanyWide
5000	CC	CompanyConfidential
7000	TS	Trade Secret

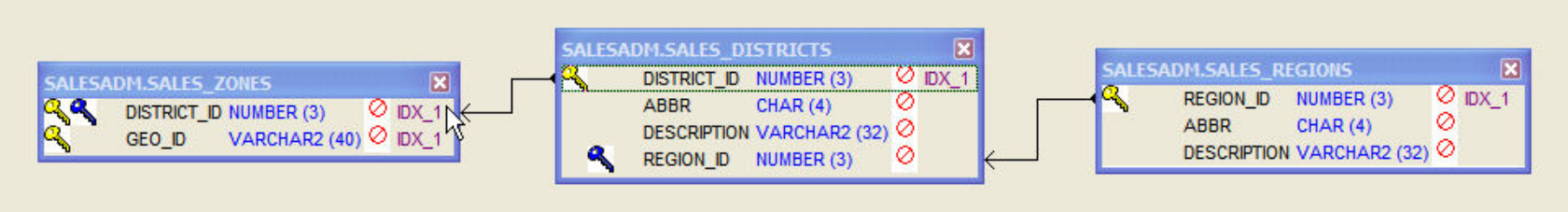
Primjer implementacije OLS

Policy labele	
Label ID	**Label Tag**
10000	UN
10100	UN:AC
10200	UN:SA
10300	UN:HR
10400	UN:OP
10500	UN:OE
30000	CW
30100	CW:SA:T
30110	CW:SA:NE
30120	CW:SA:SE
30130	CW:SA:CN
30140	CW:SA:SW
30150	CW:SA:NW
50000	CC
70000	TS

Primjer implementacije OLS



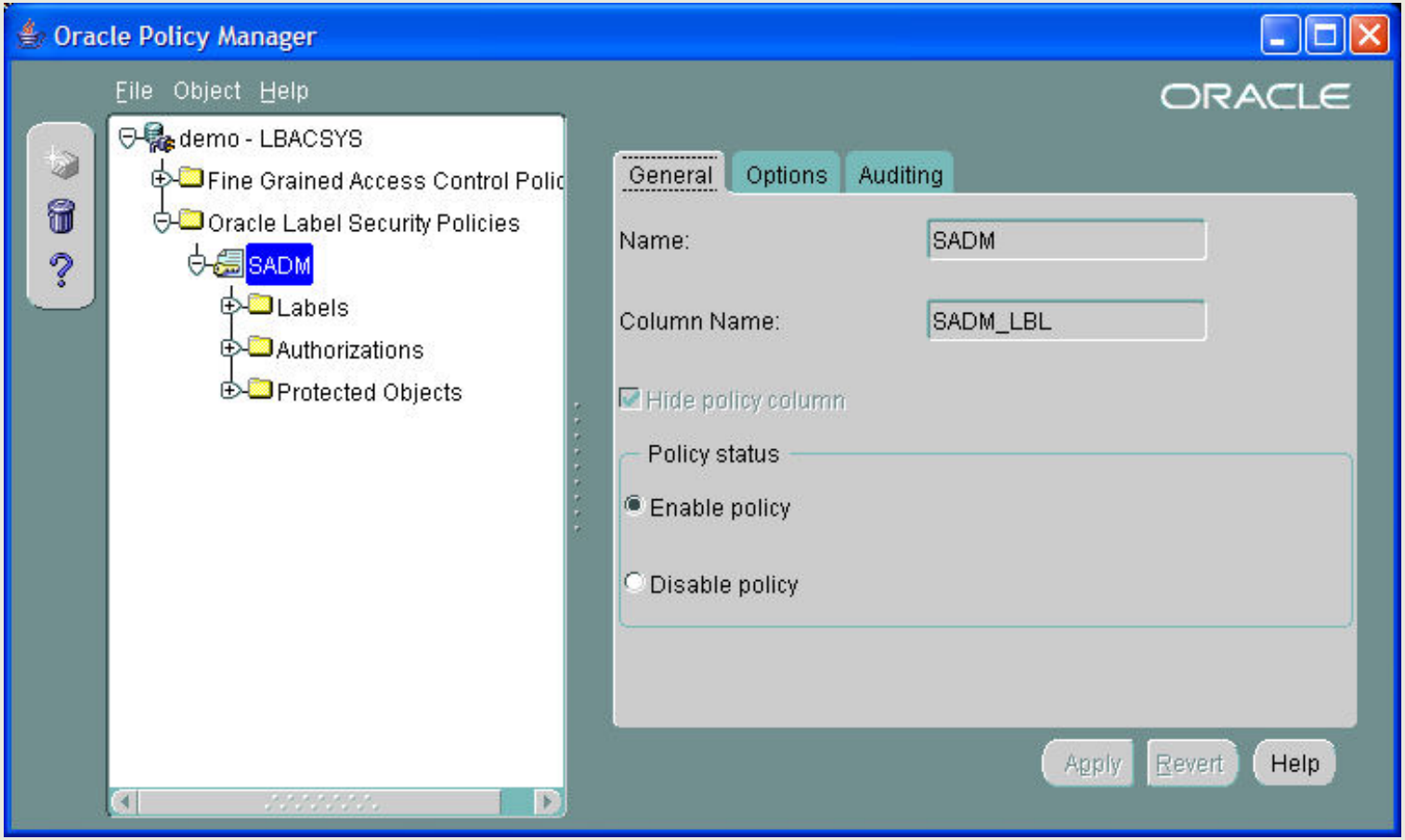
Primjer implementacije OLS



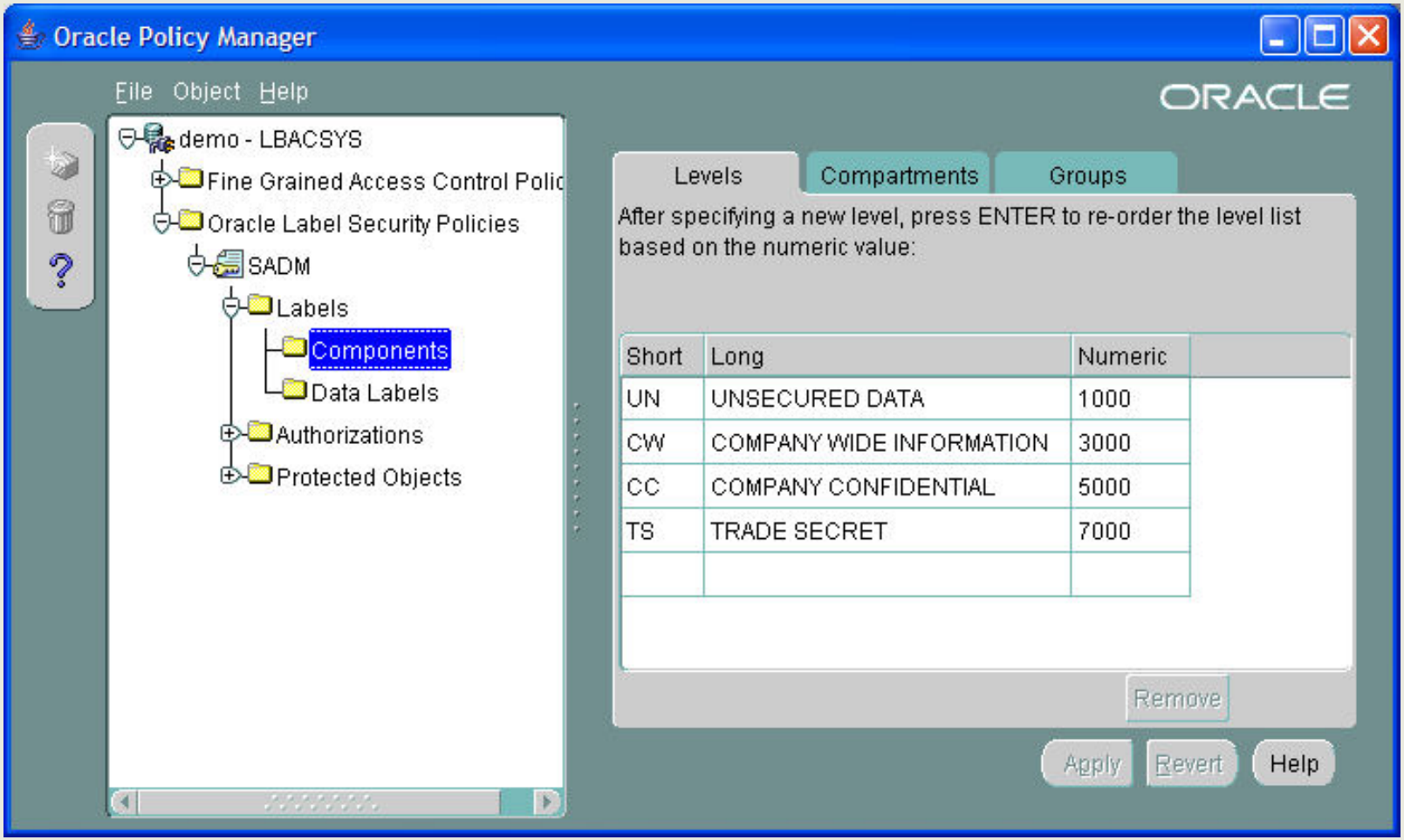
Primjer implementacije OLS

Korisnik	Funkcija	Default labela
slsmgr	Glavni menadžer prodaje	CW:SA:T
rgnmgr1	Regionalni menadžer za regiju NE	CW:SA:NE
rgnmgr2	Regionalni menadžer za regiju SE	CW:SA:SE
rgnmgr3	Regionalni menadžer za regiju CN	CW:SA:CN
rgnmgr4	Regionalni menadžer za regiju SW	CW:SA:SW
rgnmgr5	Regionalni menadžer za regiju NW	CW:SA:NW

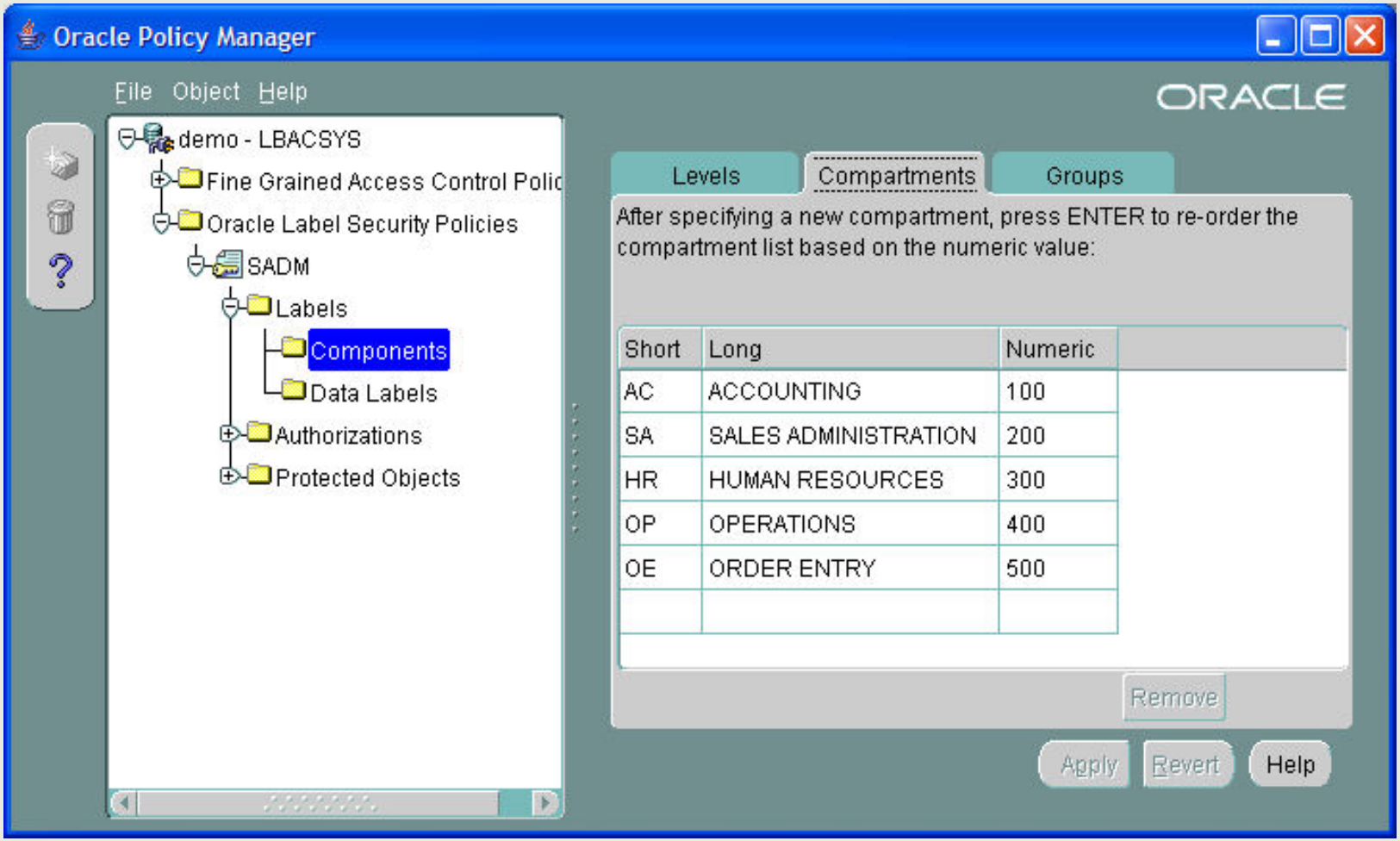
Primjer implementacije OLS



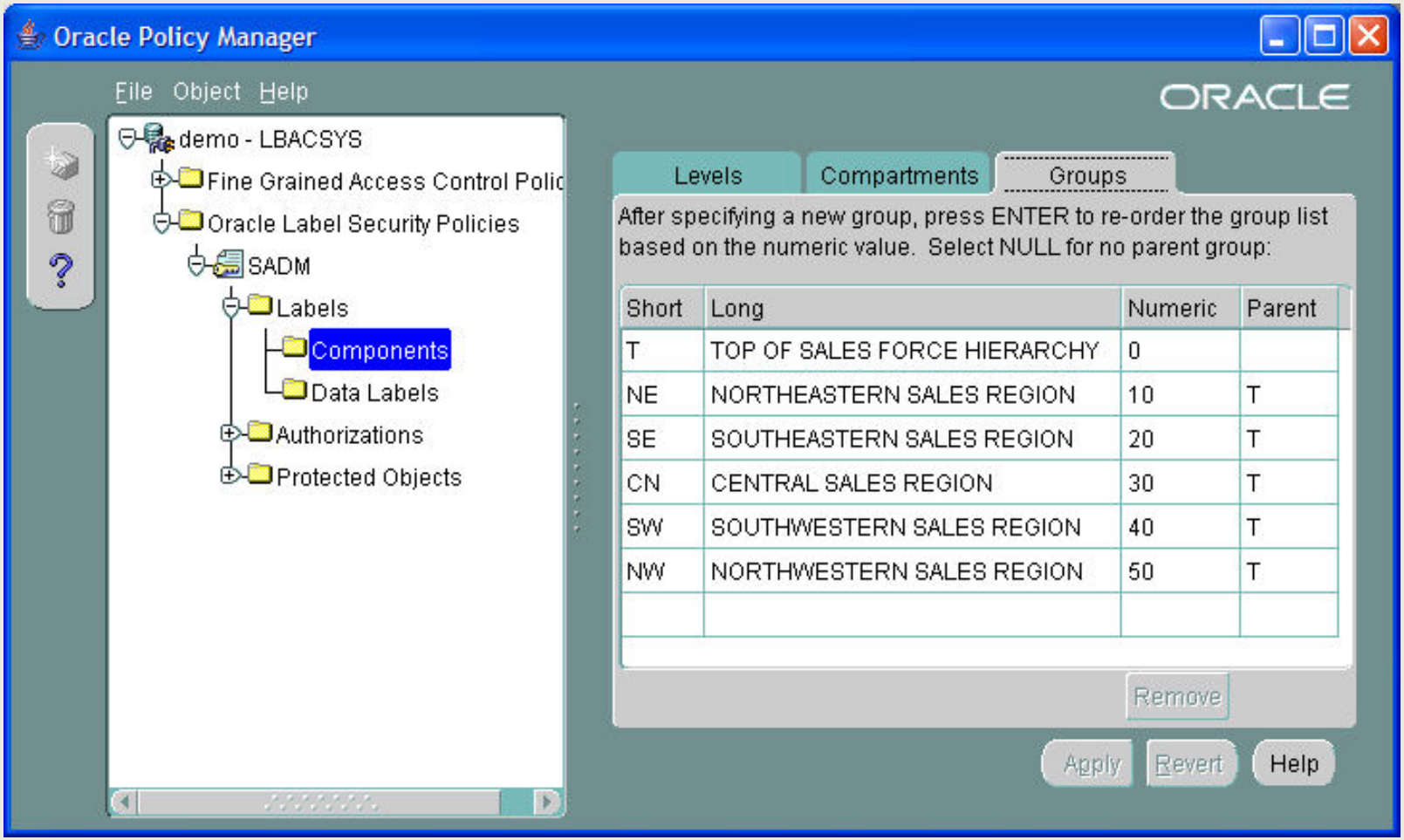
Primjer implementacije OLS



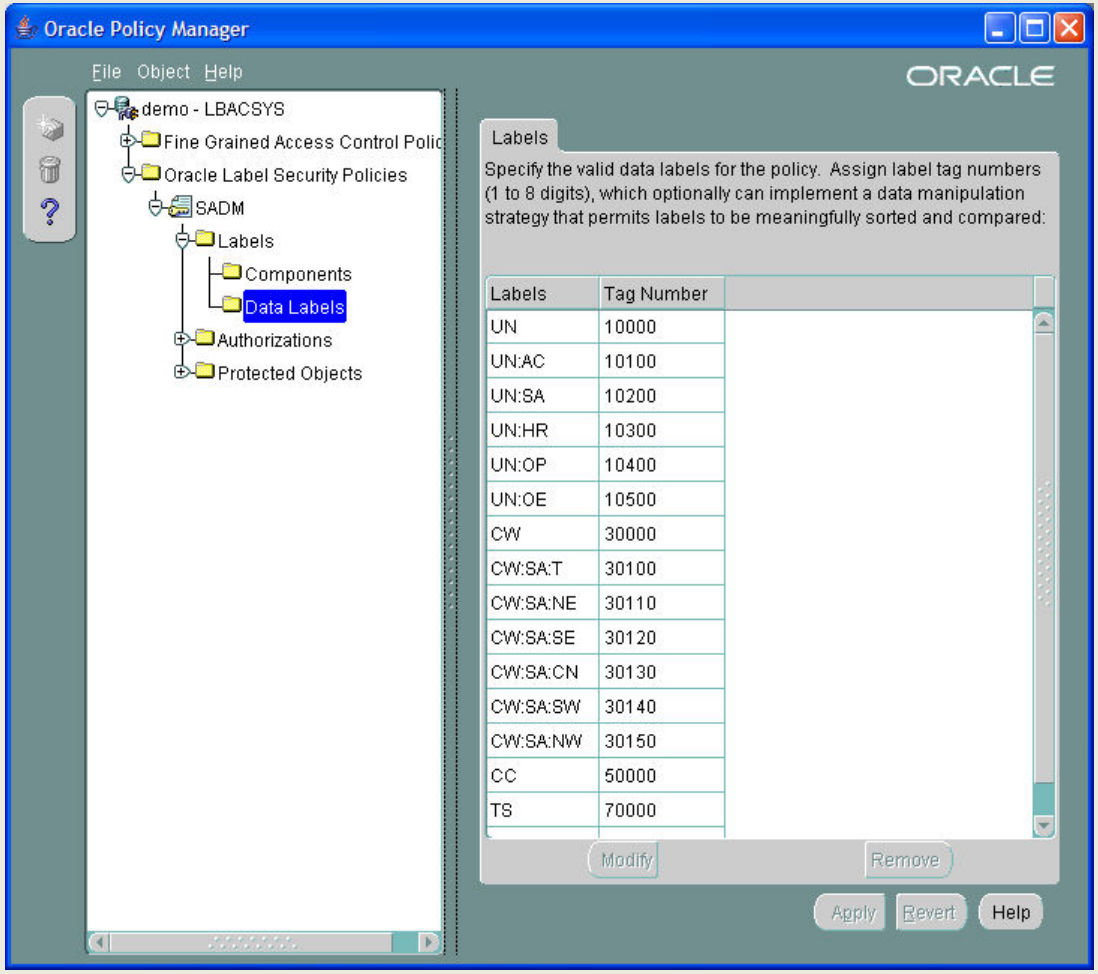
Primjer implementacije OLS



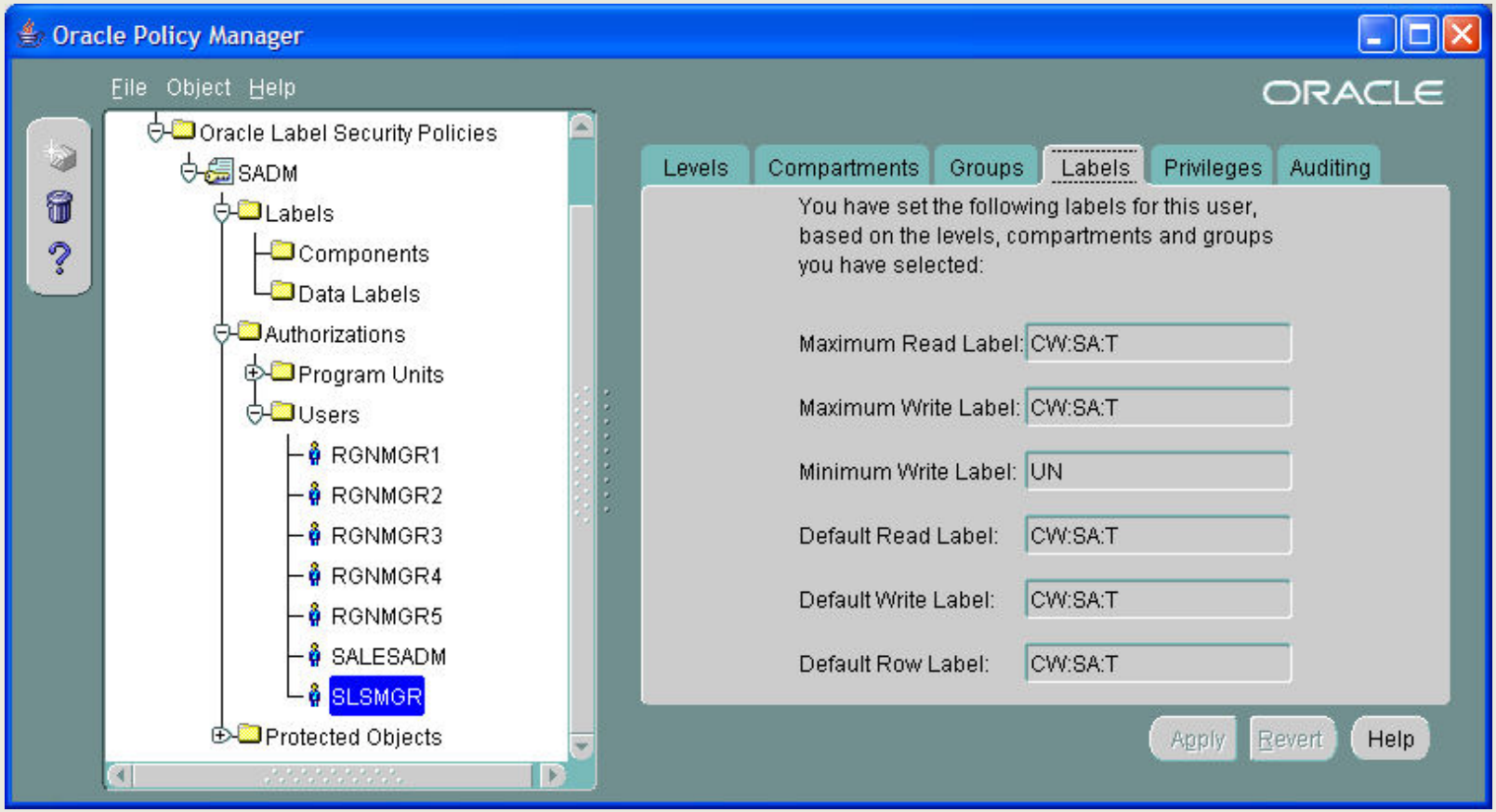
Primjer implementacije OLS



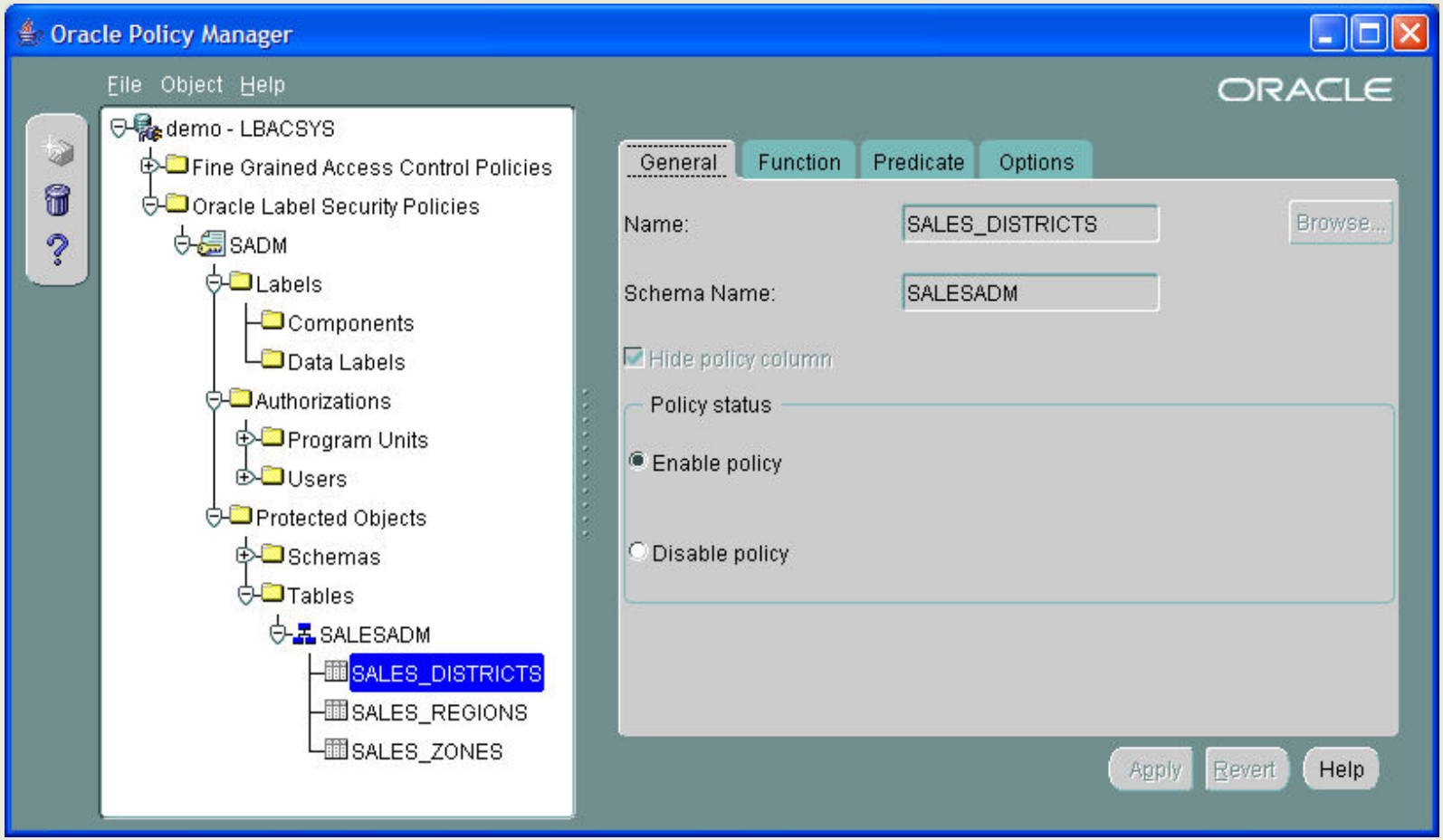
Primjer implementacije OLS



Primjer implementacije OLS



Primjer implementacije OLS



Primjer implementacije OLS

- Budući da u tablicama **sales_regions**, **sales_districts** i **sales_zones** već postoje podaci potrebno je ručno za postojeće slogove podataka upisati u kolonu **sadm_lbl** odgovarajuću labelu.
- Pri tome OLS labela treba biti upisana na taj način da slog podataka koji sadrži podatke iz jedne od regija ima labelu koja opisuje tu regiju, odnosno omogućava korisniku koji je regionalni menadžer za tu regiju čitanje tih slogova podataka.

Primjer implementacije OLS

- Na primjer za tablicu **sales_regions** labele se ažuriraju sa slijedećim SQL naredbama:

```
BEGIN
    -- Apply changes to SALES_REGIONS
    UPDATE salesadm.sales_regions
      SET sadm_lbl = CHAR_TO_LABEL('SADM', 'CW:SA:CN')
     WHERE abr = 'CN00';
    UPDATE salesadm.sales_regions
      SET sadm_lbl = CHAR_TO_LABEL('SADM', 'CW:SA:NE')
     WHERE abr = 'NE00';
    UPDATE salesadm.sales_regions
      SET sadm_lbl = CHAR_TO_LABEL('SADM', 'CW:SA:NW')
     WHERE abr = 'NW00';
    UPDATE salesadm.sales_regions
      SET sadm_lbl = CHAR_TO_LABEL('SADM', 'CW:SA:SE')
     WHERE abr = 'SE00';
    UPDATE salesadm.sales_regions
      SET sadm_lbl = CHAR_TO_LABEL('SADM', 'CW:SA:SW')
     WHERE abr = 'SW00';
    COMMIT;
END;
/
```

Primjer implementacije OLS

- Nakon toga možemo provjeriti koje podatke iz tablice **sales_regions** vide pojedini korisnici
- Kad se u bazu prijavi korisnik **slsmgr** i izvrši naredbu:

  SELECT * FROM salesadm.sales_regions;

  kao rezultat će dobiti:

  ```
  REGION_ID ABBR DESCRIPTION
  ---------- ---- ------------------------------
           1 NE00 Northeastern United States
           2 SE00 Southeastern United States
           3 CN00 Central United States
           4 SW00 Southwestern United States
           5 NW00 Northwestern United States
  ```

- Ovaj korisnik može selektirati sve podatke iz ove tablice jer je član grupe T koja je na vrhu hijerarhije grupa pa može čitati sve labele podataka

Primjer implementacije OLS

- Ako se u bazu prijavi korisnik **rgnmgr1** i izvrši isti upit kao rezultat će dobiti:

```
REGION_ID  ABBR  DESCRIPTION
---------- ----  ------------------------------
         1 NE00  Northeastern United States
```

- Ovaj korisnik je član grupe NE tako ta može čitati samo podatke koji se odnose na njegovu regiju. To također na sličan način vrijedi i za regionalne menadžere iz drugih regija.

Primjer implementacije OLS

```
CREATE OR REPLACE VIEW salesadm.sales_made
   (rgn_abbr, dst_abbr, geo_id, cust_id, total_sales, amount_sold)
AS
   SELECT
      SR.abbr,
      SD.abbr,
      SZ.geo_id,
      C.cust_id,
      SUM(SH.amount_sold),
      SUM(SH.quantity_sold)
     FROM
        salesadm.sales_regions SR,
        salesadm.sales_districts SD,
        salesadm.sales_zones SZ,
        sh.customers C,
        sh.sales SH
    WHERE SD.region_id = SR.region_id
      AND SZ.district_id = SD.district_id
      AND C.cust_state_province = SZ.geo_id
      AND C.cust_ID = SH.cust_id
    GROUP BY
      SR.abbr,
      SD.abbr,
      SZ.geo_id,
      C.cust_id
/
```

Primjer implementacije OLS

- Kad se u bazu prijavi korisnik **slsmgr** i izvrši slijedeći upit:

```
BREAK ON Rgn
 SELECT
    rgn_abbr "Rgn",
    dst_abbr "Dist",
    sum(total_sales) "Total Sales"
  FROM salesadm.sales_made
 GROUP BY rgn_abbr, dst_abbr
 ORDER BY 1,2;
```

Primjer implementacije OLS

- dobiti će slijedeći rezultat:

Rgn	Dist	Total Sales
CN00	CN10	7522340.9
	CN20	6306237.28
NE00	NE10	717164.78
	NE20	3616686.77
NW00	NW10	1161614.45
	NW20	8032676.93
SE00	SE10	9254971.59
	SE20	5328243.15
SW00	SW10	3524150.31
	SW20	5416349.56

10 rows selected.

Primjer implementacije OLS

- Kad tu istu naredbu izvrši korisnik RGNMGR1 dobiti će slijedeći rezultat:

Rgn	Dist	Total Sales
NE00	NE10	717164.78
	NE20	3616686.77

Zaključak

- opcija Oracle Enterprise Edition baze koja omogućava upravljanje dostupom korisnika do slogova podataka u tablicama
- osjetljivi se podaci mogu zaštititi od neautoriziranog pristupa
- za slogove podataka u tablici se definiraju labele u kojima je definirana osjetljivost podataka u svakom slogu
- Struktura labela se sastoji od tri komponente: razine osjetljivosti podataka, odjeljka i grupe
- Korisnike koji pristupaju podacima se temeljem organizacijske strukture tvrtke, koja može biti hijerarhijska ili u jednoj razini, podijeli u odjeljke i grupe i pridijeli im se raspon labela osjetljivosti podataka kojima mogu pristupati

Zaključak

- Za ograničavanje pristupa do podataka u tablicama se definira OLS policy s time da se ti policy mogu definirati pomoću PL/SQL procedura ili u grafičkom okruženju pomoću Oracle Policy Manager-a.
- OLS se može integrirati i sa Oracle Identity Management tako da se OLS policy mogu definirati i održavati u Oracle Internet Directory od kuda se propagiraju u sve registrirane baze
- Primjena OLS može biti kod hosting aplikacija gdje se podaci koji su vlasništvo više različitih tvrtki
- Drugo područje primjene su vojne institucije u kojima se koriste različiti povjerljivi podaci i državne institucije koje koriste različite privatne podatke o građanima koji trebaju biti zaštićeni od neovlaštenog pristupa.

informacijski inženjering

Oracle Label Security

Zoran Jovanović
tehnički direktor